WHAT IS CLAIMED IS:

1. A general finite-field multiplication method for performing $A \times B = C$ from finite-field elements A and B and a polynomial p(x) to obtain a finite-field element C, the method comprising:

a step of generating a parallel column-based matrix vector for expanding A into a matrix form and sequentially generating each element in each column of said A matrix, wherein the elements have values of $A, A\alpha, A\alpha^2 \Lambda\ A\alpha^{m-1}$, respectively; and

a step of a parallel column-based vector multiplication operation for directly multiplying each element of each column of the matrix A, that is generated sequentially, with the vector B, and all the multiplication results are accumulated so as to acquire the vector C.

2. The general finite-field multiplication method as claimed in claim 1, wherein in the step of generating a parallel column-based matrix vector, the multiplication operation of two bits is accomplished by AND operation, and the addition operation is accomplished by XOR operation.

3. The general finite-field multiplication method as claimed in claim 2, wherein in the step of generating a parallel column-based matrix vector, a latch operation is performed for latching each element in each column of said matrix A, each column in matrix A being generated sequentially, a previous column being related to a current column, all elements of a previous column being shifted with one position upwards for being placed at a lowest position of the column, said shifted element being determined whether it is added to a un-shifted element according to the p(x), so as to generate an element of the next column.

4. The general finite-field multiplication method as claimed in claim 1, wherein in the step of parallel column-based vector multiplication operation, the multiplication operation of two bits is performed by AND operation, and the addition operation is performed by XOR operation.

5. The general finite-field multiplication method as claimed in claim 4, wherein in the step of parallel column-based vector multiplication operation, an AND operation is used to obtain a result of said column element in said matrix A multiplying with said matrix B, an XOR operation being used to complete the addition operation, a latch operation being used to latch a value after addition operation, the value being accumulated to a following multiplication value through m times so as to generate said desired C vector, where m is an integral number greater than 1.

6. The general finite-field multiplication method as claimed in claim 5, wherein m is a variable depending on the bit number to be shifted in each column for providing a programmable function.

7. A general finite-field multiplication method for performing $A \times B = C$ from finite-field elements A and B and a polynomial p(x) to obtain a finite-field element C, the method comprising:

a step of generating a parallel matrix vector for generating the values of the elements in all columns of said matrix A is at a time, wherein the values are $A, A\alpha, A\alpha^2 \Lambda\ A\alpha^{m-1}$, respectively; and

a step of parallel vector multiplication operation for multiplying matrix A with said vector B when the matrix A is generated, so as to

acquire the vector C.

8. The general finite-field multiplication method as claimed in claim 7, wherein in the step of generating a parallel matrix vector, the multiplication operation of two bits is performed by AND operation, and the addition operation is performed by XOR operation.

9. The general finite-field multiplication method as claimed in claim 8, wherein in the step of generating a parallel matrix vector, all elements of a previous column are shifted with one position upwards for being placed at a lowest position, and then the shifted element is determined whether it is added to a un-shifted element according to the p(x), so as to generate elements of a next column.

10. The general finite-field multiplication method as claimed in claim 7, wherein in the step of parallel vector multiplication operation, said multiplication operation of two bits is performed by AND operation, and the addition operation is performed by XOR operation.

11. The general finite-field multiplication method as claimed in claim 10, wherein in the step of parallel vector multiplication operation, an AND operation is used to obtain a result of a row element in said matrix A multiplying with said vector B; and then an XOR operation is used to complete the addition operation of all the results of each row element in said matrix A multiplying with said vector B, so as to generate said vector C.

12. The general finite-field multiplication method as claimed in claim 11, wherein, by changing a bit number of each column to be shifted in each column, a function of programmable bit number of finite-field

element is accomplished.

13. A general finite-field multiplier for performing $A \times B = C$ from finite-field elements A and B and a polynomial p(x) to obtain a finite-field element C, the multiplier comprising:

a parallel column-based matrix vector generator for expanding A into a matrix form and sequentially generating each element in each column of said A matrix, wherein the elements have values of $A, A\alpha, A\alpha^2 \Lambda\ A\alpha^{m-1}$, respectively; and

a parallel column-based vector multiplication operation for directly multiplying each element of each column of the matrix A, that is generated sequentially, with the vector B, and all the multiplication results are accumulated so as to acquire the vector C.

14. The general finite-field multiplier as claimed in claim 13, wherein the parallel column-based matrix vector generator performs multiplication operation of two bits by AND gates, and performs addition operation by XOR gates.

15. The general finite-field multiplier as claimed in claim 14, wherein the parallel column-based matrix vector generator has a latch for latching each element in each column of said matrix A, each column in matrix A being generated sequentially, a previous column being related to a current column, all elements of a previous column being shifted with one position upwards for being placed at a lowest position of the column, said shifted element being determined whether it is added to a un-shifted element according to the p(x), so as to generate an element of the next column.

16. The general finite-field multiplier as claimed in claim 13, wherein the parallel column-based vector multiplication operator performs multiplication operation of two bits by AND gates, and performs addition operation by XOR gates.

17. The general finite-field multiplier as claimed in claim 16, wherein the parallel column-based vector multiplication operator uses AND gates to obtain a result of said column element in said matrix A multiplying with said vector B, XOR gates being used to complete the addition operation, a latch being used to latch a value after addition operation, the value being accumulated to a following multiplication value through m times so as to generate said desired C vector, where m is an integral number greater than 1.

18. The general finite-field multiplier as claimed in claim 17, wherein the parallel column-based vector multiplication operator uses a multiplexer to change the number of bits of each finite-field element.

19. A general finite-field multiplier for performing $A \times B = C$ from finite-field elements A and B and a polynomial p(x) to obtain a finite-field element C, the multiplier comprising:

a parallel matrix vector generator for generating the values of the elements in all columns of said matrix A is at a time, wherein the values are $A, A\alpha, A\alpha^2 \Lambda\ A\alpha^{m-1}$, respectively; and

a parallel vector multiplication operator for multiplying matrix A with said vector B when the matrix A is generated, so as to acquire the vector C.

20. The general finite-field multiplier as claimed in claim 19,

wherein the parallel matrix vector generator performs multiplication operation of two bits by AND gates, and performs addition operation by XOR gates.

21. The general finite-field multiplier as claimed in claim 20, wherein the parallel matrix vector generator first shifts the elements of a previous column with one position upwards for being placed at a lowest position, and then determines whether the shifted element is added to a un-shifted element according to the p(x), so as to generate elements of a next column.

22. The general finite-field multiplier as claimed in claim 19, wherein the parallel vector multiplication operator performs multiplication operation of two bits by AND gates, and performs addition operation by XOR gates.

23. The general finite-field multiplier as claimed in claim 21, wherein the parallel vector multiplication operator uses AND gates to obtain a result of a row element in said matrix A multiplying with said vector B, and uses XOR gates to complete the addition operation of all the results of each row element in said matrix A multiplying with said vector B, so as to generate said vector C.

24. The general finite-field multiplier as claimed in claim 23, wherein, the parallel vector multiplication operator uses a multiplexer to change the number of bits of each finite-field element.